*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**
01/10/2012

**SUBJECT:**
Multiple Vulnerabilities in Adobe Reader and Acrobat Could Allow For Remote Code Execution APSB12-01)

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Adobe Reader and Acrobat that could allow an attacker to take control of the affected system. Adobe Reader allows users to view Portable Document Format (PDF) files, while Adobe Acrobat offers users additional features such as the ability to create PDF files. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

Adobe has received reports that some of these vulnerabilities are being actively exploited in the wild in limited, targeted attacks against Adobe Reader 9.x on Microsoft Windows.

**SYSTEMS AFFECTED:**
- Adobe Reader X (10.1.1) and earlier 10.x versions for Windows and Macintosh
- Adobe Reader 9.4.7 and earlier 9.x versions for Windows, Macintosh and UNIX
- Adobe Acrobat X (10.1.1) and earlier 10.x versions for Windows and Macintosh
- Adobe Acrobat 9.4.7 and earlier 9.x versions for Windows and Macintosh

**RISK:**
**Government:**
- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**
- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**DESCRIPTION:**
Adobe Reader and Acrobat are prone to multiple vulnerabilities that could allow for remote code execution. Details of these vulnerabilities are as follows:
- Four memory corruption vulnerabilities which could allow for code execution
- A heap corruption vulnerability which could lead to code execution
- A U3D memory corruption vulnerability that could lead to code execution. This vulnerability was previously reported in MS-ISAC advisory 2011-072.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

Adobe has received reports that some of these vulnerabilities are being actively exploited in the wild in limited, targeted attacks against Adobe Reader 9.x on Microsoft Windows.

**RECOMMENDATIONS:**
The following actions should be taken:

- Users of Adobe Reader 9.4.7 and earlier 9.x versions for Windows and Macintosh update to Adobe Reader 9.5.
- Users of Adobe Acrobat 9.4.7 and earlier 9.x versions for Windows and Macintosh update to Adobe Acrobat 9.5.
- Users of Adobe Reader X (10.1.1) and earlier 10.x versions for Windows and Macintosh update to Adobe Reader 10.1.2.
- Users of Adobe Acrobat X (10.1.1) and earlier 10.x versions for Windows and Macintosh update to Adobe Acrobat 10.1.2.
- Consider installing and running Adobe Reader X in Protected Mode.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources

**REFERENCES:**

**Adobe:**
http://www.adobe.com/support/security/bulletins/apsb12-01.html
http://www.adobe.com/support/security/advisories/apsa11-04.html
http://www.adobe.com/support/security/bulletins/apsb11-30.html

**CVE:**
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-2462
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4369
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4370
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4371
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4372
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4373

**SecurityFocus:**
http://www.securityfocus.com/bid/50922
http://www.securityfocus.com/bid/51092
http://www.securityfocus.com/bid/51348
http://www.securityfocus.com/bid/51349
http://www.securityfocus.com/bid/51350
http://www.securityfocus.com/bid/51351